- **Use a surge protector or uninterpretable power supply (UPS)**. Prevent potential damage to your modem and router from unexpected power surges, spikes, and lightning strikes by connecting them to a surge protector or UPS. Some models also include surge protection for phone, ethernet, and coaxial cables.
- **Disable remote management. Some routers have the capability for you to manage your home network over thelinternet**. While this does add convenience, it also increases the risk that an attacker will compromise your network. Disable remote management by default, and if you absolutely need it, be sure to enable multi-factor authentication (MFA) to use this feature.
- **Change your modem and router passwords from the default passwords to secure passwords**. Changing default passwords will prevent others from accessing the configuration, changing settings, and gaining visibility into your network.
- **Enable automatic updates and install the latest firmware**. Keeping your modem and router up to date with the latest firmware helps protect them as new vulnerabilities emerge and receive fixes.
- **Enable the router's firewall**. The firewall helps prevent the devices on your network from accessing malicious sites as well as keeps outsiders on the outside of your network.
- **Enable website filtering**. Some routers have website filtering and parental controls as added features to prevent users from accessing malicious or inappropriate websites while on your network. If your router does not have these features built in, you can set up free internet Domain Name System (DNS) filtering through services such as quad9, CleanBrowsing, or OpenDNS.
- **Reboot your modem and router at least once a month**. Malicious software can infect your router without your knowledge. Periodically reboot your modem and router to clear potentially malicious software from memory, refresh your device connections, and keep your internet connection healthy and fast.

## Secure Your Wi-Fi

- **Change the Wi-Fi network name (SSID)**. The default wireless network name is typically the brand of the router. As such, it can provide clues to outsiders as to what type of router you are using and what vulnerabilities exist. Make sure you do not use your name, home address, or other personal information in your new SSID name. For added protection, disable broadcast of the wireless network name.